

Congress Directs Revisions to Sensitive Security Information



[Congressional Record: September 28, 2006 (House)]  
 [Page H7784-H7848]

CONFERENCE REPORT ON H.R. 5441, DEPARTMENT OF HOMELAND SECURITY  
 APPROPRIATIONS ACT, 2007

Conference Report (House Rept. No. 109-699)

[...]

Sec. 525. (a) Within 30 days after enactment of this Act, the Secretary of Homeland Security shall revise Department of Homeland Security (DHS) Management Directive (MD) 11056 to provide for the following:

(1) That when a lawful request is made to publicly release a document containing information designated as sensitive security information

(SSI), the document shall be reviewed in a timely manner to determine whether any information contained in the document meets the criteria for continued SSI protection under applicable law and regulation and shall further provide that all portions that no longer require SSI designation be released, subject to applicable law, including sections 552 and 552a of title 5, United States Code;

(2) That sensitive security information that is three years old and not incorporated in a current transportation security directive, security plan, contingency plan, or information circular; or does not contain current information in one of the following SSI categories: equipment or personnel performance specifications, vulnerability assessments, security inspection or investigative information, threat information, security measures, security screening information, security training materials, identifying information of designated transportation security personnel, critical aviation or maritime infrastructure asset information, systems security information, confidential business information, or research and development information shall be subject to release upon request unless:

(A) the Secretary or his designee makes a written determination that identifies a rational reason why the information must remain SSI; or

(B) such information is otherwise exempt from disclosure under applicable law:

Provided, That any determination made by the Secretary under clause (a)(2)(A) shall be provided to the party making a request to release such information and to the Committees on Appropriations of the Senate and the House of Representatives as part of the annual reporting requirement pursuant to section 537 of the Department of Homeland Security Appropriations Act, 2006 (Public Law 109-90; 119 Stat. 2088); and

(3) Common and extensive examples of the individual categories of SSI information cited under 49 CFR 1520(b)(1) through (16) in order to minimize and standardize judgment by covered persons in the application of SSI marking.

(b) Not later than 120 days after the date of enactment of this Act, the Secretary of Homeland Security shall report to the Committees on Appropriations of the Senate and the House of Representatives on the progress that the Department has

made in implementing the requirements of this section and of section 537 of the Department of Homeland Security Appropriations Act, 2006 (Public Law 109-90; 119 Stat. 2088).

(c) Not later than one year from the date of enactment of this Act, the Government Accountability Office shall report to the Committees on Appropriations of the Senate and the House of Representatives on DHS progress and procedures in implementing the requirements of this section.

(d) That in civil proceedings in the United States District Courts, where a party seeking access to SSI demonstrates that the party has substantial need of relevant SSI in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the information by other means, the party or party's counsel shall be designated as a covered person under 49 CFR Part 1520.7 in order to have access to the SSI at issue in the case, provided that the overseeing judge enters an order that protects the SSI from unauthorized or unnecessary disclosure and specifies the terms and conditions of access, unless upon completion of a criminal history check and terrorist assessment like that done for aviation workers on the persons seeking access to SSI, or based on the sensitivity of the information, the Transportation Security Administration or DHS demonstrates that such access to the information for the proceeding presents a risk of harm to the nation: Provided, That notwithstanding any other provision of law, an order granting access to SSI under this section shall be immediately appealable to the United States Courts of Appeals, which shall have plenary review over both the evidentiary finding and the sufficiency of the order specifying the terms and conditions of access to the SSI in question: Provided further, That notwithstanding any other provision of law, the Secretary may assess a civil penalty of up to \$50,000 for each violation of 49 CFR Part 1520 by persons provided access to SSI under this provision.

[...]

Section 525. The conferees continue and modify a provision proposed by the House and Senate requiring DHS to revise, within 30 days after enactment, its management directive on Sensitive Security Information (SSI) to among other things, provide for the release of certain SSI information that is three years old unless the Secretary makes a written determination that identifies a rational reason why the information must remain SSI. The conferees expect this rational reason written determination to identify and describe the specific risk to the national transportation system. The provision also contains a mechanism for SSI to be used in civil judicial proceedings if the judge determines that is needed. The conferees expect that a party will be able to demonstrate undue hardship to the judge if equivalent information is not available in one month's time. The conferees expect the criminal history records check and terrorist threat assessment on the persons seeking access to SSI in civil proceedings to be identical to that conducted for aviation workers. The conferees further expect any DHS demonstration of risk or harm to the nation in a judicial proceeding include a description of the specific risk to the national transportation system. This is consistent with demonstrations made for classified information.

washingtonpost.com

**TSA Secrecy Rules Eased**); } //-->  
Advertisement

Thursday, October 12, 2006; A25

Congress has ordered the Department of Homeland Security to ease secrecy rules at the Transportation Security Administration, helping families of victims of the Sept. 11, 2001, attacks who have sued to unearth security practices before then.

A \$34.8 billion homeland security spending bill signed by President Bush last week requires the department to release "security sensitive information" that is more than three years old and is not part of existing plans or certain categories, barring "a rational reason" cited by Secretary Michael Chertoff that it should remain secret.

Congress ordered that SSI-designated evidence be released in civil cases with some restrictions if required by a judge, unless such access "presents a risk of harm to the nation."

In a statement, Michael Low of Batesville, Ark., thanked Congress on behalf of 9/11 Families United to Bankrupt Terrorism "for telling TSA not to misuse the term 'national security' as an excuse to hide documents that are of no use to would-be terrorists but instead contain information embarrassing to our government and the airlines." Low is the father of Sara Low, a flight attendant on American Airlines Flight 11.

About 50 survivors' suits targeting airlines and security firms are before the U.S. Southern District of New York, as is a broader case against terrorist financing.

The White House opposed the change, which it said would impose "an ongoing, burdensome review process."

Steven Aftergood, director of the Federation of American Scientists' project on government secrecy, called the legislation "surprising" and a "welcome gesture by Congress to push back against expanding secrecy."

SSI includes airport security plans, vulnerability assessments and technical specifications of screening equipment, but TSA's definition is open-ended. The program has been invoked to withhold information about bomb scares at airports and to drop cases against screeners charged with stealing from passengers, for example.

It has raised concerns that local law enforcement may not be able to issue reports about incidents at airports, or that passengers stopped by security officers may not learn why they were stopped.

-- Spencer S. Hsu

© 2007 The Washington Post Company

NMU (10/11/2006): New law will alter handling of sensitive information

<http://www.rcfp.org/news/2006/1011-foi-newlaw.htm>

NEWS MEDIA UPDATE · WASHINGTON, D.C. · Freedom of Information · Oct. 11, 2006

## New law will alter handling of sensitive information

- After three years, an agency must justify the continued withholding of anything labeled "sensitive security information" under a law passed last week.

Oct. 11, 2006 · A little-noticed provision of a bill to fund the Department of Homeland Security signed by President Bush last week makes significant changes to how agencies handle unclassified information that is withheld from the public for security reasons.

While the rules apply to all agencies within the department, the new law targets the Transportation Security Administration's use of "sensitive security information," or SSI, a label affixed to information deemed too much of a security threat to release.

Critics have accused the TSA of overusing the designation to shield itself from criticism.

The new law creates a procedure for reviewing SSI after three years to determine if the reasons for withholding the information from the public are still valid. It also establishes a mechanism for utilizing SSI in civil federal court cases, allowing lawyers who obtain proper security clearances to view the information.

Under the new rules, if a public requester seeks access to a piece of information labeled SSI that is three years old, it must be "reviewed in a timely manner" to see if it still warrants SSI protection. To make the determination, an agency official will see if it falls within one of a dozen categories of information that remains protected. If the information falls outside the categories, the information must be released unless the agency can cite a "rational reason" for its continued protection.

The three-year review period brings the handling of SSI more in line with that of classified information, which prior to this new law had the distinction of being both more potentially damaging than SSI if released, but also more likely to be released eventually because it is subject to an automatic review process.

Steven Aftergood, the director of the Project on Government Secrecy for the Federation of American Scientists, said that while no one disputes that certain TSA practices and policies must be kept secret out of security concerns, he thinks the agency has overused the SSI designation.

His group recently published a study of the categories of information withheld from the public under SSI that has led him to believe the scope of the TSA's designations exceed the scope of national security.

"It is a sizeable number of documents ... and you wonder if it is all necessary," he said. "A lot of it is security related and maybe is justified in its SSI designation. The rest of it is a little hard to tell."

Whether the three-year review period will result in greater openness remains to be seen. But the new procedure for handling SSI in civil court cases could have an immediate impact in one high-profile lawsuit.

Some family members and other victims of the Sept. 11 terrorist attacks have sued airlines and the government over the security procedures in place on that day for protecting airliners. The case has proceeded at a glacial pace because the TSA, citing SSI rules, has refused to disclose much of the information sought by the plaintiffs' lawyers in that case.

Under the new law, lawyers can access some SSI if they can show a "substantial need" and are willing to undergo an extensive background check.

*(Department of Homeland Security Appropriations Act, 2007) — NW*